In the Claims

Amend claims 1-13 (following the format of the claims as presented herein, including insertion of new lines and indentations where applicable), and add new claims 14-61 as follows:

Sub. B29

1. (Amended) A method [for establishing] of processing a message for use in cryptographic communications comprising the steps of:

developing a composite number, n, as a product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ where k is an integer greater than 2, and $p_1, p_2, \ldots p_k$ are distinct random prime numbers; and

encoding a plaintext message word signal M to a ciphertext word signal C, where M corresponds to a number representative of [a] the message and

$0 \leq M \leq n-1$,

[n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ where k is an integer greater than 2, $p_1, p_2, \ldots p_k$ are distinct prime numbers, and] where C is a number representative of an encoded form of the plaintext message word signal M such that

$C \equiv M^e \pmod{n}$, and [, wherein said encoding step comprises the step of:

transforming said message word signal M to said ciphertext word signal C whereby

$C=M^e \pmod{n}$]

where e is a number relatively prime to $(p_1 -1)\cdot(p_2 -1)\cdot\ldots\cdot(p_k-1)$.

2. (Amended) The method according to claim 1, comprising the further step of:

establishing a number, d, as a multiplicative inverse of

$e(\mathrm{mod}(\mathrm{lcm}((p_1 -1), (p_2 -1), \ldots, (p_k -1))))$; and

decoding the ciphertext word signal C to the plaintext message word signal M[, wherein said decoding step comprises the step of: transforming said ciphertext word signal C] where[by:]

[$M=C^d \pmod{n}$] $M \equiv C^d \pmod{n}$

[where d is a multiplicative inverse of e(mod(lcm((p$_1$ -1), (p$_2$ -1), . . . , (p$_k$ -1))))].

3. (Amended) A method [for transferring] of processing a message signal M_i for use in a communications system having j terminals, [wherein] each terminal [is] being characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$, where i=1, 2, . . . , j, and [wherein] the message signal M_i [corresponds] corresponding to a number representative of a message-to-be-transmitted from the i^{th} terminal, the method comprising the steps of:

computing n_i where n_i is a composite number of the form

[$n_i = P_{i,1} \cdot p_{i,2} \cdot, \ldots, \cdot p_{i,k}$] $n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$

where k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to [lcm($p_{i,1}$ -1, $p_{1,2}$ -1, $p_{i,k}$ -1)] lcm($p_{i,1}$ -1, $p_{i,2}$ -1, . . . $p_{i,k}$ -1), and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

e_i (mod(lcm(($p_{i,1}$ -1), ($p_{i,2}$ -1), . . . , ($p_{i,k}$ -1))));[,

comprising the step of:]

encoding a digital message word signal [M_A]M_1 for transmission from a first terminal (i=1[A]) to a second terminal (i=2[B]), said encoding step including the sub-step of:

transforming said message word signal [M_A]M_1 to one or more message block word signals [M_A"]M_1", each block word signal [M_A"]M_1" corresponding to a number representative of a portion of said message word signal [M_A]M_1 in the range $0 \leq M_A" \leq n_2 - 1$ [$0 \leq M_A" \leq n_B - 1$],

transforming each of said message block word signals [M_A"]M_1" to a ciphertext word signal [C_A, C_A corresponding] C_1 that corresponds to a number representative of an encoded form of said message block word signal [M_A"]M_1"[,] where[by:]

[$C_A \equiv M_A"^{eB} \pmod{n_B}$] $C \equiv M_1"^{e_1} \pmod{n_2}$.

4. (Amended) A cryptographic communications system comprising:

a communication [medium] channel adapted for transmitting a ciphertext word signal C that relates to a transmit message word signal M;

[an]encoding means coupled to said channel and adapted for transforming [a] the transmit message word signal M to [a] the ciphertext word signal C using a composite number, n, where n is a product of the form

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$

k is an integer greater than 2, and

$p_1, p_2, \ldots p_k$ are distinct random prime numbers [and for transmitting C on said channel],

where the transmit message word signal M corresponds to a number representative of a message and

$0 \leq M \leq n-1$ [where n is a composite number of the form

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$

where k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and]

where the ciphertext word signal C corresponds to a number representative of an [enciphered] encoded form of said message through a relationship of the form[and corresponds to]

$C \equiv M^e \pmod{n}$, and

where e is a number relatively prime to lcm(p1 -1, p2 -1, . . . , pk -1); and

[a]decoding means coupled to said channel and adapted for receiving the ciphertext word signal C from said channel and for transforming the ciphertext word signal C to a receive message word signal M' where M' corresponds to a number representative of a [deciphered] decoded form of the ciphertext word signal C [and corresponds to] through a relationship of the form

$M' \equiv C^d \pmod{n}$

where d is selected from the group consisting of [the] a class of numbers equivalent to a multiplicative inverse of

$e(\text{mod}(\text{lcm}((p_1 -1), (p_2 -1), \ldots, (p_k -1))))$.

5. (Amended) A cryptographic communications system having a plurality of terminals coupled by a communications channel, [including] comprising:

a first terminal of the plurality of terminals characterized by an [associated] encoding key $E_A =(e_A, n_A)$ and a decoding key $D_A =(d_A, n_A)$,

where[in] n_A is a composite number of the form

$n_A = p_{A,1} \cdot p_{A,2} \cdot \ldots \cdot p_{A,k}$

where

k is an integer greater than 2,

$p_{A,1}, p_{A,2}, \ldots, p_{A,k}$ are distinct random prime numbers,

e_A is relatively prime to

$\text{lcm}(p_{A,1} -1, p_{A,2} -1, \ldots, p_{A,k} -1)$, and

d_A is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$e_A (\text{mod}(\text{lcm}((p_{A,1} -1), (p_{A,2} -1), \ldots, (p_{A,k} -1))))$; and[,]

[and including]a second terminal of the plurality of terminals having[, comprising:]

blocking means for transforming a first message,[-to-be-transmitted] which is to be transmitted on said communications channel from said second terminal to said first terminal, to one or more transmit message word signals M_B, where each M_B corresponds to a number representative of said message in the range

$0 \leq M_B \leq n_A -1$,

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_B to a ciphertext word signal C_B that [and for transmitting

C_B on said channel, where C_B] corresponds to a number representative of an [enciphered] encoded form of said first message [and corresponds to] through a relationship of the form

[$C_B \equiv M_B^{eA} \pmod{n_A}$] $C_B \equiv M_B^{e_A} \pmod{n_A}$,

[wherein]said first terminal having [comprises:]

decoding means coupled to said channel and adapted for receiving said ciphertext word signals C_B from said channel and for transforming each of said ciphertext word signals C_B to a receive message word signal [M_B]M'_B, and

means for transforming said receive message word signal[s] [M']M'_B to said first message, where [M']M'_B [is] corresponds to a number representative of a [deciphered] decoded form of C_B [and corresponds to] through a relationship of the form

[$M_B' \equiv C_B^{da} \pmod{n_A}$] $M'_B \equiv C_B^{d_A} \pmod{n_A}$.

6. (Amended) The system according to claim 5 wherein said second terminal is characterized by an [associated] encoding key [E_B =(e_B, n_B)]E_B =(e_B, n_B) and a decoding key [DB=(D_B, d_B)]D_B =(d_B, n_B), where[:

] n_B is a composite number of the form

$n_B = p_{B,1} \cdot p_{B,2} \cdot \ldots \cdot p_{B,k}$

where k is an integer greater than 2,

$p_{B,1}$, $p_{B,2}$, . . . $p_{B,k}$ [$P_{B,1}$, $P_{B,2}$, . . . $P_{B,k}$] are distinct random prime numbers,

e_B is relatively prime to

lcm($p_{B,1}$-1, $p_{B,2}$-1, . . . $p_{B,k}$-1), and

d_B is selected from the group consisting of [the] a class of numbers equivalent to a multiplicative inverse of

e_B (mod(lcm(($p_{B,1}$-1), ($p_{B,2}$ -1), . . . , ($p_{B,k}$ -1)))),

[wherein]said first terminal [comprises:] further having

blocking means for transforming a second message,[-to-be-transmitted] which is to be transmitted on said communications channel from said first terminal to said second terminal, to one or more transmit message word signals M_A, where each M_A corresponds to a number representative of said message in the range

$[0 \leq M_A^{eB} \pmod{n_B}]$ $0 \leq M_A \leq n_B - 1$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_A to a ciphertext word signal C_A and for transmitting C_A on said channel, [

]where C_A corresponds to a number representative of an encoded[enciphered] form of said second message [and corresponds to] through a relationship of the form

$[C_A \equiv M_A^{eB} \pmod{n_B}]$ $C_A \equiv M_A^{e_B} \pmod{n_B}$

[wherein] said second terminal [comprises;] further having

decoding means coupled to said channel and adapted for receiving said ciphertext word signals C_A from said channel and for transforming each of said ciphertext word signals to a receive message word signal $[M_A']M'_A$, and

means for transforming said receive message word signals $[M_A]M'_A$ to said message, [

]where [M'] M'_A corresponds to a number representative of a [deciphered] decoded form of C_A [and corresponds to] through a relationship of the form

$[M_A' \equiv C_A^{dB} \pmod{n_B}]$ $M'_A \equiv C_A^{d_B} \pmod{n_B}$.

7. (Amended) A method [for establishing] of processing a message for use in cryptographic communications, comprising the steps of:

developing a composite number, n, as a product of at least 3 whole number factors greater than one, the factors being distinct random prime numbers; and

encoding a digital message word signal M to a [cipher text] ciphertext word signal C, where said digital message word signal M corresponds to a number representative of a message and

$0 \leq M \leq n-1$,

[where n is a composite number having at least 3 whole number factors greater than one, the factors being distinct prime numbers, and]

where said ciphertext word signal C corresponds to a number representative of an encoded form of said message [word M,] through a relationship of the form

[wherein said encoding step comprises the step of:

transforming said message word signal M to said ciphertext word signal C whereby]

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \pmod{n}$$

where e and a_e, a_{e-1}, . . ., a_0 are numbers.

8. (Amended) [In the] A method according to claim 7 wherein said encoding step further includes the step of

transforming said digital message word signal M to said cipertext word signal C by the performance of a first ordered succession of inveritble operations on M, [the further step of:]

and wherein the method further comprises the step of:

decoding said cipertext word signal C to said digital message word signal M by the performance of a second ordered succession of invertible operations on C, where each of the invertible operations of said second ordered succession is the inverse of a corresponding one of said first ordered succession, and where[in] the order of said invertible operations in said second ordered succession is reversed with respect to the order of corresponding invertible operations in said first ordered succession.

9. (Amended) A communication system for [transferring] processing message signals [M_i], comprising:

[ ]j terminals including first and second terminals[stations], each of the j [stations]terminals being characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$[ ], where i=1,2, . . . j, [and wherein

M_i corresponds to a number representative of a message signal to be transmitted from the i^{th} terminal,] each of the j terminals being adapted to transmit a particular one of the message signals where an i^{th} terminal corresponds to an i^{th} message signal M_j, and

$0 \leq M_i \leq n_i - 1$,

n_i [is] being a composite number of the form

[$n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$] $n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to

$\text{lcm}(p_{i,1}-1, p_{i,2}-1, \ldots p_{i,k}-1)$, and

d_i is selected from the group consisting of the class of numbers equivalent

to a multiplicative inverse of

$e_i \pmod{\text{lcm}((p_{i,1}-1), (p_{i,2}-1), \ldots, (p_{i,k}-1))}$;

said[a] first terminal [one of the j terminals] including

means for encoding a digital message word signal [M_A] M_1 [for transmission] to be transmitted from said first terminal (i=1[A]) to [a]said second terminal [one of the j terminals] (i=2[B]), said encoding means [for] transforming said digital message word signal [M_A]M_1 to a signed message word signal [M_{As}] M_{1s} using a relationship of the form [, M_{1s} corresponding to a number representative of an encoded form of said message word signal M_A,

whereby:]

$$[M_{As} \equiv M_A^{dA} \pmod{n_A}] \; M_{1s} \equiv M_1^{d_1} \pmod{n_1}.$$

10. (Amended) The communication system of claim 9 further comprising:

means for transmitting said [signal]signed message word signal [M_{As}] M_{1s} from said first terminal to said second terminal, [and wherein]

said second terminal [includes] including

means for decoding said signed message word signal [M_{As}] M_{1s} to said digital message word signal [M_A,] M_1 using a relationship of the form [said second terminal including:]

$$M_1 \equiv M_{1s}^{e_1} (\mathrm{mod}\, n_1)$$

[means for transforming said signed message word signal M_{As} to said message word signal M_A, whereby

$$M_A \equiv M_{As}^{eA} (\mathrm{mod}\, n_A)].$$

11. (Amended) A communications system for transferring a message signal [M_i], the communications system comprising:

[ ]j communication stations including first and second stations, each of the j communication stations being characterized by an encoding key $E_i=(e_i, n_i)$ and a decoding key $D_i=(d_i, n_i)$, where i=1, 2,. . . , j, [and wherein M_i corresponds to a number representative of a message signal to be transmitted from the i^{th} terminal,] each of the j communication stations being adapted to transmit a particular one of the message signals where an i^{th} communication station corresponds to an i^{th} message signal M_i, and

$0 \leq M_i \leq n_i - 1$

n_i [is] being a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to lcm($p_{i,1}$ -1,$p_{i,2}$ -1, . . . ,$p_{i,k}$ -1), and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

e_i (mod(lcm(($p_{i,1}$ -1), ($p_{i,2}$ -1), . . . , ($p_{i,k}$ -1)))).

[a]said first station [one of the j communication stations] including

means for encoding a digital message word signal [M_A] M_1 [for transmission] to be transmitted from said first station [one of the j communication stations] (i=1[A]) to [a] said second station [one of the j communication stations] (i=2[B]),

means for transforming said digital message word signal [M_A] M_1 to one or more message block word signals [M_A'] M_1", each block word signal [M_A'] M_1" being a number representative of a portion of said message word signal [M_A']M_1 in the range

$0 \leq M_1'' \leq n_2 - 1$ [$0 \leq M_A \leq n_B - 1$], and

means for transforming each of said message block word signals [M_A"] M_1" to a ciphertext word signal C_1 using a relatinship of the form [C_A , C_A corresponding to a number representative of an encoded form of said message block word signal M_A", whereby:]

$[C_A \equiv M_A''^{Eb} \pmod{n_B}]$ $C_1 \equiv M''^{e_2}_1 \pmod{n_2}$.

12. (Amended) The communications system of claim 11 further comprising:

means for transmitting said ciphertext word signals C_1 from said first [terminal] station to said second [terminal] station, [and]

wherein said second [terminal] station includes

means for decoding said ciphertext word signals C_1 to said message block word signals [MA] M_1" using a relationship of the form[, said second terminal including:

means for transforming each of said ciphertext word signals C_A to one of said message block word signals M_A", whereby

$M_A'' \equiv C_A^{Db} \pmod{n_B}$] $M''_1 \equiv C_1^{d_2} \pmod{n_2}$, and

means for transforming said message block word signals [M_A''] $\underline{M_1''}$ to said message word signal [M_A]$\underline{M_1}$.

13. (Amended) [In a] A communications system, [including] comprising:

a first station; and

[and] a second [communicating] station[s inter]connected to the first station for communications therebetween,

the first communicating station having

encoding means for transforming a transmit message word signal M to a ciphertext word signal C where transmit message word signal M corresponds to a number representative of a message and

$0 \leq M \leq n-1$

[where] n [is] being a composite number formed as a product of [having] at least 3 whole number factors greater than one, the factors being distinct random prime numbers, and

where the ciphertext word signal C corresponds to a number representative of an [enciphered] encoded form of said message through a relationship of the form [and corresponds to]

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \pmod{n}$$

where e and a_e, a_{e-1}[-1], . . . , a_0 are numbers; and

means for transmitting the ciphertext word signal C to the second [communicating] station.

New Claims:

14. A method of processing a message for use in cryptographic communications comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

computing a composite number, n, as a product of the k distinct random prime numbers; and

encoding a plaintext message data M to a ciphertext message data C using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

15. The method according to claim 14, comprising the further step of:

establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$$; and

decoding the ciphertext message data C to the plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$.

16. A method of processing a message for use in cryptographic communications comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of

$d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

computing a composite number, n, as a product of the k distinct random prime numbers;

obtaining a ciphertext message data *C*; and

decoding the ciphertext message data *C* to a plaintext message data *M* using a relationship of the form $M \equiv C^d \pmod{n}$.

17. The method according to claim 16, comprising the further step of:

encoding the plaintext message data *M* to the ciphertext message data *C*, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

18. A method of processing a message for use in cryptographic communications comprising the steps of:

selecting a public key portion *e*;

developing *k* distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \ldots p_k-1$, is relatively prime to the public key portion *e*;

establishing a private key portion *d* by a relationship to the public key portion *e* of the form

$d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

computing a composite number, n, as a product of the k distinct random prime numbers;

encoding a plaintext message data *M* with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d \pmod{n}$, where $0 \leq M \leq n-1$.

19. The method of claim 18 further comprising the step of:

decoding the signed message M_s with the public key portion e to produce the plaintext message data *M* using a relationship of the form $M \equiv M_s^e \pmod{n}$.

20. A method for increasing the efficiency of a cryptographic process, comprising the steps of:

selecting a public key portion *e*;

developing *k* distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion *e*;

computing a composite number, n, as a product of the k distinct random prime numbers; and

encoding a plaintext message data *M* to a ciphertext message data *C*, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$,

whereby a computational speed of the cryptographic process is increased.

Q 30

21. The method according to claim 20, comprising the further step of:

establishing a private key portion *d* by a relationship to the public key portion *e* in the form of

$$d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$$; and

decoding the ciphertext message data *C* to the plaintext message data *M* using a relationship of the form $M \equiv C^d \pmod{n}$.

22. A method for increasing the efficiency of a cryptographic process, comprising the steps of:

selecting a public key portion *e*;

developing *k* distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion *e*;

establishing a private key portion *d* by a relationship to the public key portion *e* in the form of

$$d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$$;

computing a composite number, n, as a product of the k distinct random prime numbers;

obtaining a ciphertext message data *C*; and

decoding the ciphertext message data *C* to a plaintext message data *M* using a relationship of the form $M \equiv C^d \pmod{n}$,

whereby a computational speed of the cryptographic process is increased.

23. The method according to claim 22, comprising the further step of:

encoding the plaintext message data *M* to the ciphertext message data *C*, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

C30

24. The method according to claim 20, wherein p and q are a pair of prime numbers the product of which equals n, and wherein the k distinct random prime numbers are each smaller than p and q, whereby for a given length of n it takes fewer computational cycles to find and check the K distinct random prime numbers that it takes to find and check the pair of prime numbers p and q.

25. The method according to claim 22, wherein p and q are a pair of prime numbers the product of which equals n, and wherein the k distinct random prime numbers are each smaller than p and q, whereby for a given length of n it takes fewer computational cycles to find and check the K distinct random prime numbers that it takes to find and check the pair of prime numbers p and q.

26. The method according to claim 24, wherein the developing and computing steps can be performed for n that is more than 600 digits long faster than heretofore possible with only the pair of prime numbers p and q.

27. The method according to claim 25, wherein the developing, computing and encoding steps can be performed for n that is more than 600 digits long faster than heretofore possible with only the pair of prime numbers p and q.

28. The method according to claim 14, wherein p and q are a pair of prime numbers the product of which equals n, and wherein the k distinct random prime numbers are each smaller than p and q, whereby for a given length of n it takes fewer computational cycles to find and check the K distinct random prime numbers that it takes to find and check the pair of prime numbers p and q.

C 30

29. The method according to claim 28, wherein the developing and computing steps can be performed for n that is more than 600 digits long faster than heretofore possible with only the pair of prime numbers p and q.

30. The method according to claim 16, wherein p and q are a pair of prime numbers the product of which equals n, and wherein the k distinct random prime numbers are each smaller than p and q, whereby for a given length of n it takes fewer computational cycles to find and check the K distinct random prime numbers that it takes to find and check the pair of prime numbers p and q.

31. The method according to claim 30, wherein the developing and computing steps can be performed for n that is more than 600 digits long faster than heretofore possible with only the pair of prime numbers p and q.

32. The method according to claim 18, wherein p and q are a pair of prime numbers the product of which equals n, and wherein the k distinct random prime numbers are each smaller than p and q, whereby for a given length of n it takes fewer computational cycles to find and

check the K distinct random prime numbers that it takes to find and check the pair of prime numbers p and q.

33. The method according to claim 32, wherein the developing and computing steps can be performed for n that is more than 600 digits long faster than heretofore possible with only the pair of prime numbers p and q.

34. The method according to claim 14, wherein a message processed in accordance with the method is compatible with two-prime RSA public key cryptography.

35. The method according to claim 14, wherein a message processed in accordance with the method is compatible with two-prime RSA public key cryptography.

36. The method according to claim 16, wherein a message processed in accordance with the method is compatible with two-prime RSA public key cryptography.

37. The method according to claim 18, wherein a message processed in accordance with the method is compatible with two-prime RSA public key cryptography.

38. The method according to claim 20, wherein message data processed in accordance with the method is compatible with two-prime RSA public key cryptography.

39. The method according to claim 22, wherein message data processed in accordance with the method is compatible with two-prime RSA public key cryptography.

40. A cryptography method for local storage of data by a private key owner, comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1} (\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$$;

computing a composite number, n, as a product of the k distinct random prime numbers that are factors of n, where only the private key owner knows the factors of n;

encoding plaintext data M to ciphertext data C for the local storage, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

41. The cryptography method in accordance with claim 40, further comprising the step of:

decoding the ciphertext data C from the local storage to the plaintext data M using a relationship of the form $M \equiv C^d \pmod{n}$.

42. A cryptographic communications system, comprising:

a plurality of stations;

a communications medium; and

a host system adapted to conduct encrypted communications with the plurality of stations via the communications medium, the host system including

at least one cryptosystem responsive to encryption and/or decryption requests from the host system, the cryptosystem being configured for

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to a public key portion e that is associated with the host system,

computing a composite number, n, as a product of the k distinct random prime numbers,

encoding a plaintext message data M producing therefrom a ciphertext message data C to be communicated via the host system, the encoding using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$,

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\text{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$; and

decoding a ciphertext message data C' communicated via the host producing therefrom a plaintext message data M' using a relationship of the form $M' \equiv C'^{d} \pmod{n}$, where C' and M' can be respectively C and M.

Q30

43. A system for processing a message used in cryptographic communications, comprising:

a bus; and

a cryptosystem operatively coupled to and receiving from the bus encryption and decryption requests, the cryptosystem being capable of

providing a public key portion e,

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \ldots p_k-1$, is relatively prime to the public key portion e,

computing a composite number, n, as a product of the k distinct random prime numbers,

encoding a plaintext form of a first message M to produce a ciphertext form of the first message C using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$,

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\text{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$, and

decoding the ciphertext form of a second message C' to produce the plaintext form of the second message M' using a relationship of the form $M' \equiv C'^{d} \pmod{n}$, the first and second messages can be one and the same.

44. The system of claim 42, wherein the at least one cryptosystem includes

a plurality of exponentiators configured to operate in parallel in developing respective subtask values corresponding to the message.

G30

45. The system of claim 42, wherein the at least one cryptosystem includes

a processor,

a data-address bus,

a memory operatively coupled to the processor via the data-address bus,

a data encryption standard (DES) unit operatively coupled the memory and the processor via the data-address bus,

a plurality of exponentiator elements operatively coupled to the processor via the DES unit, the plurality of exponentiator elements being configured to operate in parallel in developing respective subtask values corresponding to the message.

46. The system of claim 45, wherein the memory and each of the plurality of exponentiator elements has its own DES unit that encrypts message data received/returned from/to the processor.

47. The system of claim 45, wherein the memory is partitioned into address spaces addressable by the processor including secure, insecure and exponentiator elements address spaces, and wherein the DES unit that is coupled to the processor is configured to recognize the secure and exponentiator elements address spaces and to automatically encrypt message data therefrom before it is provided to the exponentiator elements, the DES unit being bypassed when

the processor is accessing the insecure memory address spaces, the DES unit being further configured to decrypt encrypted message data received from the memory before it is provided to the processor.

48. The system of claim 45, wherein the at least one cryptosystem meets FIPS (Federal Information Processing Standard) 140-1 level 3.

C 30

49. The system of claim 45, wherein the processor maintains in the memory the public key portion e and the composite number n with its factors $p_1, p_2, \ldots p_k$.

50. A system for processing a message used in cryptographic communications, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encryption and decryption requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encryption and decryption requests, each encryption request providing a plaintext message M to be encrypted, each encryption request can additionally provide a public key that includes an exponent e and a representation of a modulus n in the form of its k distinct random prime number factors $p_1, p_2, \ldots p_k$, where $k \geq 3$, or the processor can obtain the public key from the memory,

constructing subtasks to be executed by the exponentiator elements for producing respective ones of the subtask values, $C_1, C_2, \ldots C_k$, and

forming a ciphertext message C from the subtask values $C_1, C_2, \ldots C_k$.

51. The system of claim 50 wherein each one of the subtasks $C_1, C_2, \ldots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{e_i} (\text{mod } p_i)$, where $M_i \equiv M (\text{mod } p_i)$, and $e_i \equiv e (\text{mod } p_i - 1)$, where i=1, 2, ... k.

52. A system for processing a message used in cryptographic communications, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encryption and decryption requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encryption and decryption requests, each encryption/decryption request providing a plaintext/ciphertext message *M/C* to be encrypted/decrypted and can additionally provide a public/private key that includes an exponent *e/d* and a representation of a modulus *n* in the form of its *k* distinct random prime number factors $p_1, p_2, \ldots p_k$, where $k \geq 3$, or the processor can obtain the public/private key from the memory,

constructing subtasks to be executed by the exponentiator elements for producing respective ones of the subtask values, $M_1, M_2, \ldots M_k / C_1, C_2, \ldots C_k$, and

forming the ciphertext/plaintext message *C/M* from the subtask values $C_1, C_2, \ldots C_k / M_1, M_2, \ldots M_k$.

53. The system of claim 52 wherein when produced each one of the subtasks $C_1, C_2, \ldots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{e_i} (\text{mod } p_i)$, where $C_i \equiv C (\text{mod } p_i)$, and $e_i \equiv e (\text{mod } p_i - 1)$, where i=1, 2, ... k.

54. The system of claim 52 wherein when produced each one of the subtasks $M_1, M_2, \ldots M_k$ is developed using a relationship of the form $M_i \equiv C_i^{d_i} (\mathrm{mod}\, p_i)$, where $M_i \equiv M (\mathrm{mod}\, p_i)$, and $d_i \equiv d (\mathrm{mod}\, p_i - 1)$, where i=1, 2, ... k.

55. The system of claim 54, wherein the private key exponent d relates to the public key exponent e via $d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$.

56. A system for processing a message used in cryptographic communications, comprising:

means for selecting a public key portion e;

means for developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, ... p_k-1, is relatively prime to the public key portion e;

means for establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$;

means for computing a composite number, n, as a product of the k distinct random prime numbers;

means for obtaining a ciphertext message data C; and

means for decoding the ciphertext message data C to a plaintext message data M using a relationship of the form $M \equiv C^d (\mathrm{mod}\, n)$.

57. The system according to claim 56, further comprising:

means for encoding the plaintext message data M to the ciphertext message data C, using a relationship of the form $C \equiv M^e (\mathrm{mod}\, n)$, where $0 \leq M \leq n$-1.

58. A system for processing a message used in cryptographic communications, comprising:

means for selecting a public key portion e;

means for developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

means for establishing a private key portion d by a relationship to the public key portion e of the form $d \equiv e^{-1}(\text{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

means for computing a composite number, n, as a product of the k distinct random prime numbers;

means for encoding a plaintext message data M with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d \pmod{n}$, where $0 \leq M \leq n-1$.

A30

59. The system of claim 58 further comprising the step of:

means for decoding the signed message M_s with the private key portion e to produce the plaintext message data M using a relationship of the form $M \equiv M_s^e \pmod{n}$.

60. The system of claim 57, wherein the system can conduct encrypted communications with other public key cryptography system that encrypt/decrypt data using a modulus value equal to n independent of the k distinct prime numbers.

61. The system of claim 59, wherein the system can conduct encrypted communications with other public key cryptography systems that encrypt/decrypt data using a modulus value equal to n independent of the k distinct prime numbers.